AUDIT PROCEDURES

for

REGISTRATION AUTHORITY OFFICE

(Operating under IDRBT CA Office)

INF/PKI/06.03/261/30.0

IDRBT,
Castle Hills, Road No. 1
Masab Tank, Hyderabad,
Andhra Pradesh – 500057, India
Ph: 040 23294217, 19 & 21
Fax: 040 23535157
Email: cahelp@idrbt.ac.in

A Certifying Authority (CA) is a body that fulfills the need for trusted third party services in electronic commerce by issuing Digital Certificates that attest to some fact about the subject of the Certificate. A Certificate is a digitally signed statement by a CA that provides independent confirmation of an attribute claimed by a person offering a Digital Signature. As a Certifying Authority licensed by the Controller of Certifying Authorities (CCA), Government of India, IDRBT CA issues, administers and revokes Digital Certificates of subscribers who are members of INFINET.

The Certificate management involves interaction between entities (called 'end entities' or 'Users') identified by Certificates and CA. These interactions include operations such as registration for certification, Certificate retrieval, Certificate renewal, Certificate revocation and key back-up & recovery. In order to provide maximum operational flexibility, the interactions with end entities or Users are handled by a separate service called Registration Authority (RA).

The RA is an entity dedicated to user registration and accepts requests for digital certificates. User registration is the process of collecting user information and verifying user credentials which is then used to register a user according to the policy of IDRBT CA. The credibility of a certificate issued by IDRBT CA depends on the authentication process adopted by the RA. The Registration Authority Office consists of at least one RA Administrator and at least one RA Officer. The RA Officials verify the certificate/revocation request(s), corresponding credentials of the user, digitally sign the request(s) and submit to IDRBT CA for issuance/revocation of certificate(s). Banks may appoint multiple RA Administrators and RA Officers under the same organization as also may set up multiple RA Offices.

As the RA Office is part and parcel of IDRBT CA, they are to get audited as per the Information Technology Act 2000, Rules and Regulations for Certifying Authorities 2001. IDRBT CA advises the RA Offices to carry out audit as per CCA guidelines issued from time to time.

Audit Requirements

Given below is the audit checklist to be maintained by the RA Office:

1. Certificate Request Details

   Checklist of certificate requests as per Annexure-1. This list is to be maintained every six months and ***soft copy has to sent by email digitally signed by RA Administrator to*** cahelp@idrbt.ac.in with subject as "Audit document for xxxxx RA Office during the period of DD/MM/YYYY to DD/MM/YYYY".

   Note: The email should contain the soft copy of the Annexure -1 as attachment.

- Subscriber application form filled and duly signed by subscriber and approved by RA Officer/RA Administrator as per Appendix-3 of Rules and Guidelines for RA Office document.

- Copy of documents (PAN Card and Aadhar, Passport/Voter's ID/Driving License/Bank's ID Card) essential for verifying subscriber credentials according to Class of certificate.

- Acknowledgment of user-id and login password from subscriber.

- While issuing SSL Certificates, the guidelines issued by CCA that has been circulated to all RAs are to be strictly followed.

2. Revocation Details

   Checklist of Revocation requests as per Annexure-2. This list is to be maintained once in every six months
   and ***soft copy by email digitally signed by RA Administrator to*** cahelp@idrbt.ac.in with subject as "Audit document for xxxxx RA Office during the period of DD/MM/YYYY to DD/MM/YYYY".

   Note: The email should contain the soft copy of the Annexure – 2 as attachment.

   - Certificate Revocation/Suspension form as per Appendix-4 of Rules and Guidelines for RA Office document.

3. Copy of Master Agreement as per Appendix-2 of Rules and Guidelines for RA Office document. In case of multiple RA Offices in the same organization, the **copy of the agreement** should be kept at each RA Office location.

4. Copy of communication with subscriber in paper/electronic media (if any).

5. Copy of communication with IDRBT CA office in paper/electronic media.

6. Financial records should be maintained as per Annexure-3A and 3B as applicable.

7. Details of transfer/termination of duty/revocation of RA Officials' .

ANNEXURE – 1

Details of Certificate Requests

(Put Y for Yes, N for No & NA for Not Applicable)

S. No.	User ID	Date of Creation of User ID	Request No.	Date of Receipt of online Request in RA Office	Class of Cert.	Type of Cert.	Date of Release of request to CA Office	Rejected (Y/N/NA)	Cert. S.No.	Expiry Date (dd/mm/yy)	Remarks

ANNEXURE – 1A

Details of Certificate Requests (Sample)

[redacted]	User ID	Date of Creation of User ID	Re No.	Da eipt ne t in ice	Class of ert.	Type of ert.	Date of of request to CA Office	Rejected (Y/N/NA)	Cert. No.	Expiry Date (dd/mm/yy)	Remarks
1	123	18/05/03	10	22 3	1	US	22/5/03	N	0A5	22/05/05	
2	456	19/05/03	10	23 3	2	UE	25/5/2003	Y		N.A.	Invalid ed by the ber
3	895	22/05/03	10	24 3	2	SS	26/5/03	N	045	27/05/05	Expired 2004

TIPS

1. Use ***1*** for ***Class 1***, ***2*** for ***Class 2***, ***3*** for ***Class 3*** in the class of cert. column.
2. Use ***WS for Web Server***, ***US*** for ***User Signing***, ***UE*** for ***User Encryption***, ***SS*** for ***System Certificate***, ***i***n the Type of Cert. column.
3. Fill the *Cert. S.No.* Column after the certificate is issued to the Subscriber.
4. Make use of the report generation facility provided in the IDRBT CA Reports Option.

ANNEXURE – 2

The details of digital certificates whose keys have been compromised

(Put Y for Yes & N for No)

S. No.	User ID	Cert. S.No.	Class of Cert.	Type of Cert.	Revocation Request No.	Reason for revocation	Initiated By		Remarks
							Subscriber (Y/N)	RA (Y/N)	

ANNEXURE – 2A

The details of digital certificates whose keys have been compromised (Sample)

S. No.	User ID	Cert. S.No.	Class of Cert.	Type of Cert.	Revocation Request No.	Reason for revocation	Initiated By		Remarks
							Subscriber (Y/N)	RA (Y/N)	
1	**123**	**0AA**	**1**	**US**	**234**	**Key compromise**	**Y**	**N**	**Token lost**
2	**456**	**0DB**	**2**	**US**	**254**	**Unspecified**	**N**	**Y**	**Retired from the service**

TIPS

1. Use ***1*** for ***Class 1***, ***2*** for ***Class 2***, ***3*** for ***Class 3*** in the class of cert. column.
2. Use ***WS for Web Server***, ***US*** for ***User Signing***, ***UE*** for ***User Encryption***, ***and SS for System Certificate*** in the Type of Cert. column.
3. Fill the *Cert. S.No.* column with respect to the certificate issued to the Subscriber.
4. Make use of the reports options available in the menu after logging in as RA Administrator / RA Officer.

ANNEXURE – 3A

Payment format for Digital Certificate (for Fresh requests)

From : _ _ / _ _ / 20_ _ To: _ _ / _ _ / 20_ _

(1US – Class 1 Signing Cert., 1UE – Class 1 Encryption Cert., 2US – Class 2 Signing Cert., 2UE – Class 2 Encryption Cert., 3US – Class 3 User Signing Cert., 3UE – Class 3 User Encryption Cert., 3SS – Class 3 Server System Cert., 3WS – Class 3 Web Server Cert.) Please write request numbers separated by comma(,).

	Request Numbers	**Total no. of Requests**	**Total (Rs.)** *(Total No. of requests* **x** *Rate of the certificate)*
1US			
1UE			
2US			
2UE			
2SS			
3SS			
3WS			
TOTAL			

ANNEXURE – 3B

Payment format of RA Office (for Renewal requests)

From : _ _ / _ _ / 20_ _ To: _ _ / _ _ / 20_ _

(1US – Class 1 Signing Cert., 1UE – Class 1 Encryption Cert., 2US – Class 2 Signing Cert., 2UE – Class 2 Encryption Cert., 3US – Class 3 User Signing Cert., 3UE – Class 3 User Encryption Cert., 3SS – Class 3 Server System Cert.,, 3WS – Class 3 Web Server Cert.) Please write request numbers separated by comma(,).

	Request Numbers	**Total no. of Requests**	**Total (Rs.)** *(Total No. of requests* **x** *Rate of the renewal certificate)*
1US			
1UE			
2US			
2UE			
2SS			
3SS			
3WS			
TOTAL			